CloudSmart Playbook

California Department of Technology

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As the State of California is digitally transforming to better service Californians, and re-envisioning the Cloud, the California Department of Technology (CDT) is revising Cloud services, allowing for more sophisticated adoption approaches to support state entities on their Cloud journeys. This playbook was designed as a long-term strategy to support California state entities on their journey to the adoption of cloud technology and to achieve enhanced security, cost savings, and streamlined delivery of digital government services.

This Playbook provides a catalog of guidance on adoption topics, describing an overarching strategy and tactical approaches to achieving them while emphasizing enhanced security, architecture, workforce, and procurement measures to deliver an improved, collaborative approach to Cloud integration regardless of where you are on the journey.

This Playbook represents our commitment to the belief in and value of collaboration.

We firmly believe a collaborative approach offers value by:

- Generating diverse solutions from shared ideas
- Maximizing resources
- Increasing civic engagement across state agencies, departments, and entities

1.1 Why Cloud?

The opportunity for cloud is to remove friction and enable a truly connected government – aligning state entities to become truly customer-centric and digitally enabled that are engineered for customer satisfaction. Measurable benefits such as cost flexibility, quicker deployments, metered resource utilization, and self-service have spurred initial adoption.

Organizations must understand that some challenges exist in optimally moving and running on cloud platforms and quickly discover that simply plugging into the cloud will not achieve digital transformation and by thinking differently – these challenges can be overcome to accelerate the delivery of outcomes using cloud platforms. Below are the essential attributes to sustainably deliver value and outcomes using cloud platforms.

1.2 What is Cloud?

Government follows guidance from the National Institute of Standards and Technology (NIST). NIST has identified five essential characteristics of cloud — and in order to be properly considered "cloud," any third-party system must meet them. The five essentials are:

1. Scale resources, like server time or network storage on your own, whenever you want — you don't need to work with an IT department.
2. Gives you a variety of ways to access your resources outside of your organization's network: mobile phones, tablets, laptops, workstations, etc.
3. Multiple users access a shared set of physical and virtual resources based on demand.
4. Gives you the ability to scale your resources quickly, both outward and inward.
5. Automatically track your resource usage so that you pay for only what you actually use.

NIST also defines four cloud deployment models: public clouds, private clouds, community clouds, and hybrid clouds. A cloud deployment model defines where the infrastructure for the deployment resides and who has control over that infrastructure. Each cloud deployment model satisfies different organizational needs, so it's important that you choose a model that will satisfy the needs of your organization. An emerging deployment model is multi cloud.

Moreover, each cloud deployment model has a different value proposition and different costs associated with it. To make an informed decision, organizations need to be aware of the characteristics of each environment.

Public clouds allow multiple organizations — from both the public and private sectors — to access the same computing resources. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. This drives innovation, as well as economies of scale. It's a mistake to assume public clouds aren't secure; many public clouds are FedRAMP authorized and/or StateRamp authorized and supported by large security teams. And industry relies on these types of clouds to keep their information safe. Unless the information you need to store is sensitive, a public cloud could easily meet your security requirements. If you do need additional data safeguarding, some cloud providers offer special government-only clouds that are "public" while still meeting higher levels of security and compliance.

Advantages

- Hyper scalability
- Pay-as-you-go cost model
- Self-service with automation

Disadvantages

- Shared resources
- Infrastructure controlled by third party
- Reskilling and upskilling resources

Private clouds offer the same characteristics as a public cloud, but are only available to a single agency, housed in on-premises datacenter or third-party managed datacenter. Computing resources can be governed, owned, and operated by the same organization. Private clouds rarely offer the same benefits as a public cloud, and lose the efficiency and scale offered from pooled resources, rapid elasticity, and expansion.

Advantages

- Organization specific
- High degree of security and level of control
- Ability to choose your resources (ie. specialized hardware)

Disadvantages

- Lack of elasticity and capacity to scale (bursts)
- Limited pay-as-you-go cost model
- Requires a significant amount of engineering effort

Community clouds are cloud resources shared by multiple (usually just a few) organizations with similar interests and requirements — for example, defense, intelligence, or medical communities. It's effectively a middle ground between a public and private cloud; some of the innovation and cost savings are still available because some or all of the resources are shared. Community clouds may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Advantages

- Community specific or purpose built
- Automation
- Balance of convenience and security

Disadvantages

- Requires a significant amount of engineering effort

Hybrid clouds are a composition of two or more distinct cloud deployment models (private, community, or public) that remain unique entities but are working together by standard or proprietary technology that enables data and application portability, coordinated by a cloud broker that federates data, applications, user identity, security, and other details. Hybrid cloud providers are responsible for managing resources based on agency requirements. As with a private cloud model, it's important to make sure cloud services make the most of cloud's benefits.

Advantages

- Cost Effective
- Reduce risk of service disruption
- Scalability/Flexibility
- Balance of convenience, performance, and security

Disadvantages

- More complex
- Requires additional engineering effort
- Availability of resources with requisite skill sets

2. What is not Cloud?

In NIST's definition, the essential characteristics of cloud computing include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Anything that doesn't fulfill these characteristics, deployment models, or service models as outlined by NIST wouldn't be considered cloud computing according to their definition.

A traditional on-premises data center infrastructure would be an example of a non-cloud solution according to the NIST definition. Here's why:

- **Lack of On-Demand Self-Service:** In a traditional data center setup, provisioning resources often require manual intervention from IT staff. Users typically can't independently provision resources on-demand through a self-service interface.

- **Limited Network Access:** Access to resources in an on-premises data center may be limited to users within the organization's physical network, unlike the broad network access characteristic of cloud computing, where resources can be accessed over the internet.

- **Limited Resource Pooling:** In a traditional data center, resources are typically dedicated to specific applications or departments, leading to underutilization of resources compared to the resource pooling characteristic of cloud computing, where resources are shared dynamically among multiple users and applications.

- **Limited Elasticity:** Scaling resources up or down in a traditional data center often requires purchasing and provisioning additional hardware, which can be time-consuming and expensive compared to the rapid elasticity characteristic of cloud computing, where resources can be scaled automatically in response to changing demand.

- **Lack of Measured Service:** In a traditional data center, it may be difficult to accurately track resource usage and allocate costs to individual users or departments compared to the measured service characteristic of cloud computing, where usage is monitored and billed based on actual consumption.

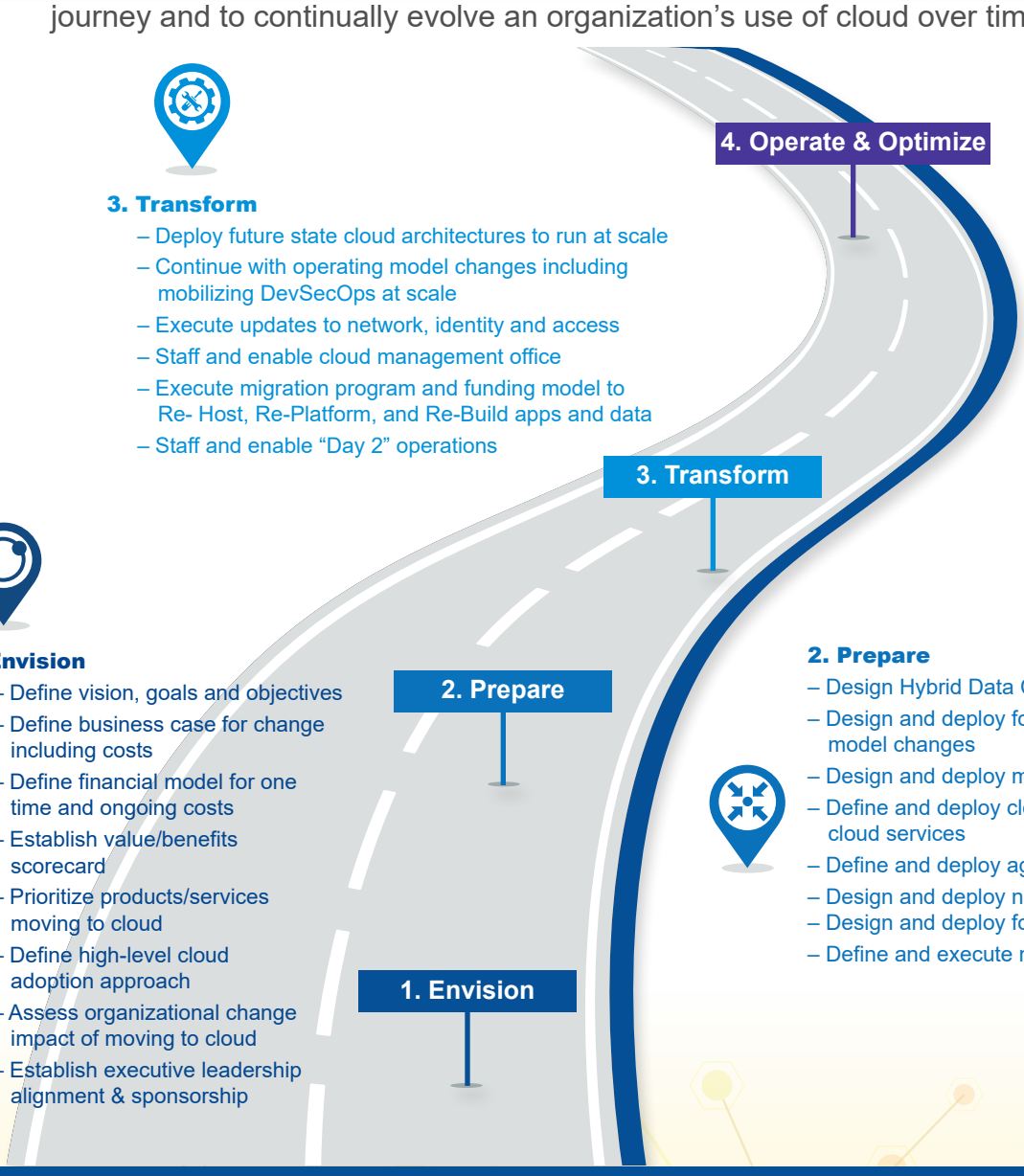
So, a traditional on-premises data center infrastructure would not meet the NIST definition of cloud computing due to its lack of these essential characteristics.

ROAD TO SUCCESS

Getting to the cloud is a journey. It doesn't happen overnight. Organizations are under increasing pressure to deliver Cloud transformation results quickly. Getting started and charting the steps is critical for success.

This general cloud journey encapsulates the cultural and behavioral change that integrates business, development, and operations teams to work together to achieve specific outcomes. It is an integration of people, tools, and process through the use of automation to quickly, frequently and reliably deliver software at a higher level of quality and at a lower cost.

Each of the four milestones on the journey map provides practical steps to jump-start your journey and to continually evolve an organization's use of cloud over time.



1. Envision
- Define vision, goals and objectives
- Define business case for change including costs
- Define financial model for one time and ongoing costs
- Establish value/benefits scorecard
- Prioritize products/services moving to cloud
- Define high-level cloud adoption approach
- Assess organizational change impact of moving to cloud
- Establish executive leadership alignment & sponsorship

2. Prepare
- Design Hybrid Data Center Strategy and Architecture
- Design and deploy foundational cloud operating model changes
- Design and deploy migration factory capabilities/strategy
- Define and deploy cloud policies and standards for using cloud services
- Define and deploy agile and security practices DevSocOps
- Design and deploy network, identity and access changes
- Design and deploy foundational cloud architectures
- Define and execute migration proof of concepts

3. Transform
- Deploy future state cloud architectures to run at scale
- Continue with operating model changes including mobilizing DevSecOps at scale
- Execute updates to network, identity and access
- Staff and enable cloud management office
- Execute migration program and funding model to Re- Host, Re-Platform, and Re-Build apps and data
- Staff and enable "Day 2" operations

4. Operate & Optimize
- Automate everything end-to-end
- Focus on reliably and securely operating at speed and scale
- Embedded policies, security, and controls in to cloud services
- Establish self-service for requesting and deploying cloud services
- Integrate monitoring, alerting and resiliency in to cloud services
- Enable charge/show back and cost optimization capabilities
- Establish Cloud advisory and brokerage for cloud services

Protect & Govern

Change & Communication

Figure 2 – Cloud Journey Roadmap

The culture and ways of working must evolve to sustainably deliver outcomes and value using cloud platforms. Enhancements to tools and Process are meaningless unless paired with a culture which fosters collaboration & continuous improvement. This must be aligned at all levels and drives organizational change. With the advent of Cloud, Agile practices, and techniques such as containerization and infrastructure as code organizations can move at market speed while maintaining quality. In order to gain the promise of agility process, tools, and culture leading organizations much shift shared responsibility for Risk and Security into a full stack organization.

Common areas of an operating model that must change to take advantage of the promises of cloud.

Figure 3 – Operating Model Changes

2.1 Planning Strategically

There are some common questions to answer when beginning the journey to the cloud. To ensure cloud integration aligns with an organization's vision and also brings value, the entity must define its cloud vision and create a clear plan and framework to realize the cloud's benefits.

Exploration

Open the hood and examine the technology portfolio to identify opportunities where cloud can deliver value

Key questions

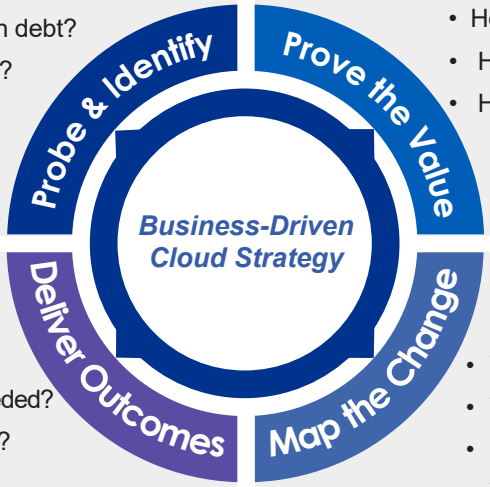
- What are the priorities that drive the vision?
- What are the business imperatives & outcomes?
- What is the state of IT and level of tech debt?
- What cloud services enable outcomes?
- What are the blockers to generating value?

Collaboration

Business and IT define the value drivers to measure and track value that enable business outcomes

Key questions

- What are the value drivers?
- What are the one-time and on-going costs?
- How do you measure the value drivers?
- How you link the value to outcomes?
- How do you communicate value?



Mobilization

Key questions

- How do we organize to get started?
- What roles, skills and capabilities are needed?
- What immediate actions to get started?
- What projects do we start with?
- How do we monitor and adjust accordingly?
- What does success look like?

Set the roadmap to build out a secure and complaint cloud ecosystem to deliver business outcomes at speed and scale

Elaboration

Key questions

- What is the path to run at speed & scale?
- What investments are needed?
- How does the operating model change?
- What new roles and skills are needed?
- Do we need to organize differently?
- Are people ready to change?

Cloud changes the ways work gets done, how work is organized and how services are delivered.

Figure 4 – Business Drivers

2.2 Cloud Adoption Strategies

There are five scenarios common to organizations considering cloud technology: Re-host, Re-Platform, Redesign, Replace and Retire. For cloud adoption, common scenarios considered are Scalability and Flexibility Needs, Cost Optimization and Efficiency, Disaster Recovery and Business Continuity Global Expansion and Accessibility. The resulting disposition is dependent upon the cloud adoption strategy, the business and, of course, the available budget and resources. The figure below is used as a general decision tree to inform strategic steps forward.

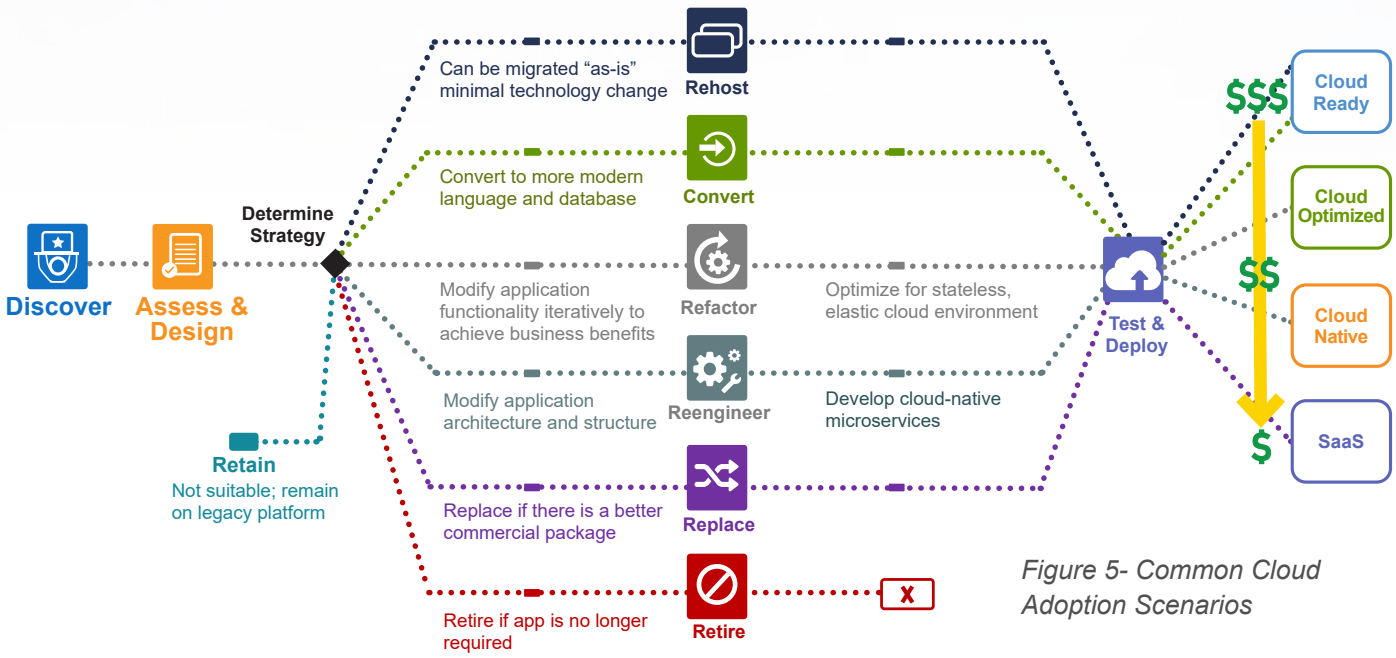


Figure 5- Common Cloud Adoption Scenarios

Re-host

Redeploy the application component to other (physical, virtual or cloud) infrastructure without recompiling, modifying the application code, or modifying its features and functions.

Re-Platform

Migrate the application component to a new runtime platform. Make minimal changes to code to adapt to the new platform, but do not change the code structure or the features and functions it provides.

Redesign

Rebuild or rewrite the application component from scratch while preserving its scope and specifications.

Replace

Eliminate the former application component altogether, and replace it, taking new requirements needs into account.

Retire

Application is no longer useful and can simply be turned off. Savings from retirement can boost the business case, direct your attention to things that the business needs.

2.3 Cloud Service Model Adoption Guides

In addition to selecting deployment model(s), appropriate service model(s) also need to be selected. NIST has defined three cloud computing service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These different cloud service models work together, the underlying infrastructure supporting the platforms, and those platforms in turn support the application software.

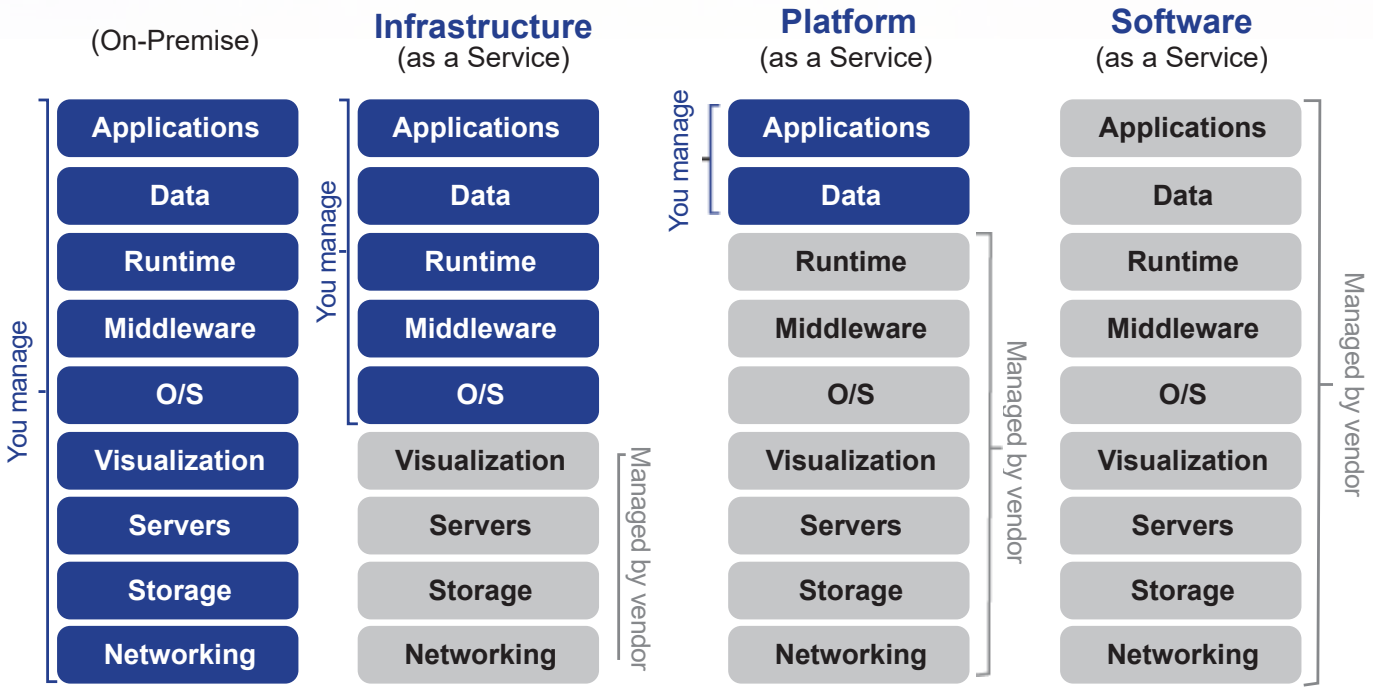


Figure 6 – Cloud Service Models

Infrastructure as a Service

IaaS is a model where a third-party supplier provides consumers with control over the deployed application and the server operating system, without managing the underlying cloud infrastructure.

Platform as a Service

PaaS is a model where a third-party supplier provides hosting services on a cloud platform and the consumer does not manage the underlying cloud infrastructure.

Software as a Service

SaaS outsources everything, including the code of the applications used. Users have very little responsibility for the application software — the provider is responsible for keeping it up to date, easy to use, or compliant. In exchange, the user has minimal control over what the application software does, how it works or when it changes/updates. SaaS solutions, unlike other cloud models, tend to be direct end-user-facing.

3. California Cloud Services

In 2023, CDT established the California Cloud Services Program, to align with the Federal Cloud Smart Strategy. CDT's California Cloud Services revolves around five key components of successful and smart cloud adoption:

Security and Compliance

Risk-based decision making, automation, and data-focused protections are the focus for improving the State's security and supportability posture. Departments moving to the Cloud must assure statewide security policies are followed for citizen and state data protection and privacy requirements. Cloud Security and Cloud Compliance is a collaborative collection of information and artifacts regarding cloud security.

Broadly, the cloud provider is responsible for "security of the cloud," while the customer is responsible for "security in the cloud." The responsibility to secure cloud resources is shared between the customer and the cloud service provider, with varying responsibilities depending on the resource type and service model. Even with this shared responsibility, state entities remain ultimately responsible for selecting and configuring cloud services commensurate with risk tolerance and regulatory requirements. The utilization of cloud services does not exempt state agencies/entities from security provisions of the SAM and SIMM.

Cloud providers strive to achieve certification of their services with various regulatory requirements (e.g., HIPAA, PCI) and demonstrate their compliance through attestations by third-party, independent audits. Certification of compliance does not apply wholly to a cloud provider, but rather the ability of specific services to be configured in a way that meets compliance requirements. It is the responsibility of the State entity to determine what regulations apply to their workloads, and then select and configure cloud services accordingly.

State systems may require compliance with the Federal Risk and Authorization Management Program, FedRAMP, as a funding condition. FedRAMP authorizes services at two levels: Moderate and High. The differences between FedRAMP Moderate and High are intended to designate cloud systems with different impact on information systems. The two basic types are formally defined in the Federal Information Processing Standards (FIPS) Publication 199. These security controls are for three objectives:

- **Confidentiality:** Information access and disclosure for protecting personal privacy and proprietary information.
- **Integrity:** Stored information is sufficiently guarded against modification or destruction.
- **Availability:** Ensuring timely and reliable access to information.

FedRAMP High has 421 security controls while Moderate has 325 security controls. For more details of the Security Controls see:

https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Controls_Baseline.xlsx

Cloud Architecture

Streamlining and standardizing Cloud architecture across the state is a priority for CDT. Uniform architecture provides enhanced public service delivery to Californians.

Additionally, it presents new opportunities for shared services, economies of scale, and efficiently managed operational costs. Scalable services can be adapted to meet changes in demand and new functionality. CDT provides cloud monitoring tools, allowing visibility to scale up and down as needed. Leveraging shared platforms promotes collaboration among the state's workforce and makes sharing valuable data less difficult.

Standardized architecture provides increased security, visibility, and compliance with state policies.

Workforce Development

Adopting cloud technologies within an organization begins with the motivation for adopting cloud computing. By far the most important factor in a cloud readiness assessment is the cultural element. Understanding the workforce implications is critical when introducing a move to a new paradigm such as cloud.

Potentially, coupled with a change-averse culture and a narrowly skilled workforce, the most sound and informed plans could go nowhere without this understanding. Organizational readiness to accept change, identify the issues, and then address them, is another critical element.

California aims to recruit, retain, and upskill fundamental statewide talent for cloud engineering and cybersecurity. Through staff development, State civil service staff are given the opportunity to provide the services needed by other state entities, reducing the dependency on non-state personnel, and presenting cost savings to the State.

State Partnerships

CDT offers a path for agencies and State entities to collaborate on the most safe and secure cloud infrastructure and will provide support to achieve consistent, maintainable, cost-efficient delivery of services. CDT will partner with state entities to tailor solutions that best meet the individual department's cloud goals and business objectives.

CDT's California Managed Cloud (CAMC) Services offers access to the various off-premises cloud services in the public cloud. This program provides customers the ability to use highly flexible, well-tested, and secure cloud infrastructure, while taking advantage of cutting-edge technologies and reducing upfront costs. CDT's CAMC provides services encompassing Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and off-premises solutions.

A sample of the services available through CAMC include: Serverless computing, various storage services, Relational Database Services (RDS), hardware, Operating Systems, and more.

Cloud Provider Interconnect

The Cloud Provider Interconnect (CPI) service is a CDT managed statewide solution that provides customers with secure direct connectivity from the CDT Data Centers to Cloud Service Providers (CSPs) such as Microsoft Azure and Amazon Web Services (AWS).

Procurement
State partners looking to procure off-premises cloud technologies will participate in the California Cloud Services Assessment (CCSA) process. The CCSA requires collaboration with CDT on cloud design and planning documentation, which ensures alignment with IT security, architecture, procurement, and workforce requirements and best practices, to meet service and business objectives. State partners can review the 3 Steps to Success for a quick guide on how the CCSA works. CDT offers contracts with the following Cloud Service Providers:

FedRAMP High Cloud Services

Amazon Web Services (AWS)

Microsoft Azure

FedRAMP Moderate Cloud Services

Amazon Web Services (AWS)

Microsoft Azure

GCP

OCI

4. Policy and Compliance

This section provides information and guidance around California's Cloud Computing policies and requirements. These modernized policies aim to align departments' cloud posture with the state's readiness requirements to reach a desired state of cloud security and architecture.

- Technology Letter 23-03: Update to Cloud Computing Policy – Cloud Smart
- SAM 4983.1: Cloud Computing Policy
- SIMM 140: Cloud Security Guide
- SIMM 141: California Cloud Smart Assessment Guide

  State entities planning to submit a California Cloud Services Assessment request can follow the instructions outlined in this guide.

5. Journey to the Cloud

Most State entities will follow a typical Cloud adoption journey, varying depending on the organization's Cloud maturity level.

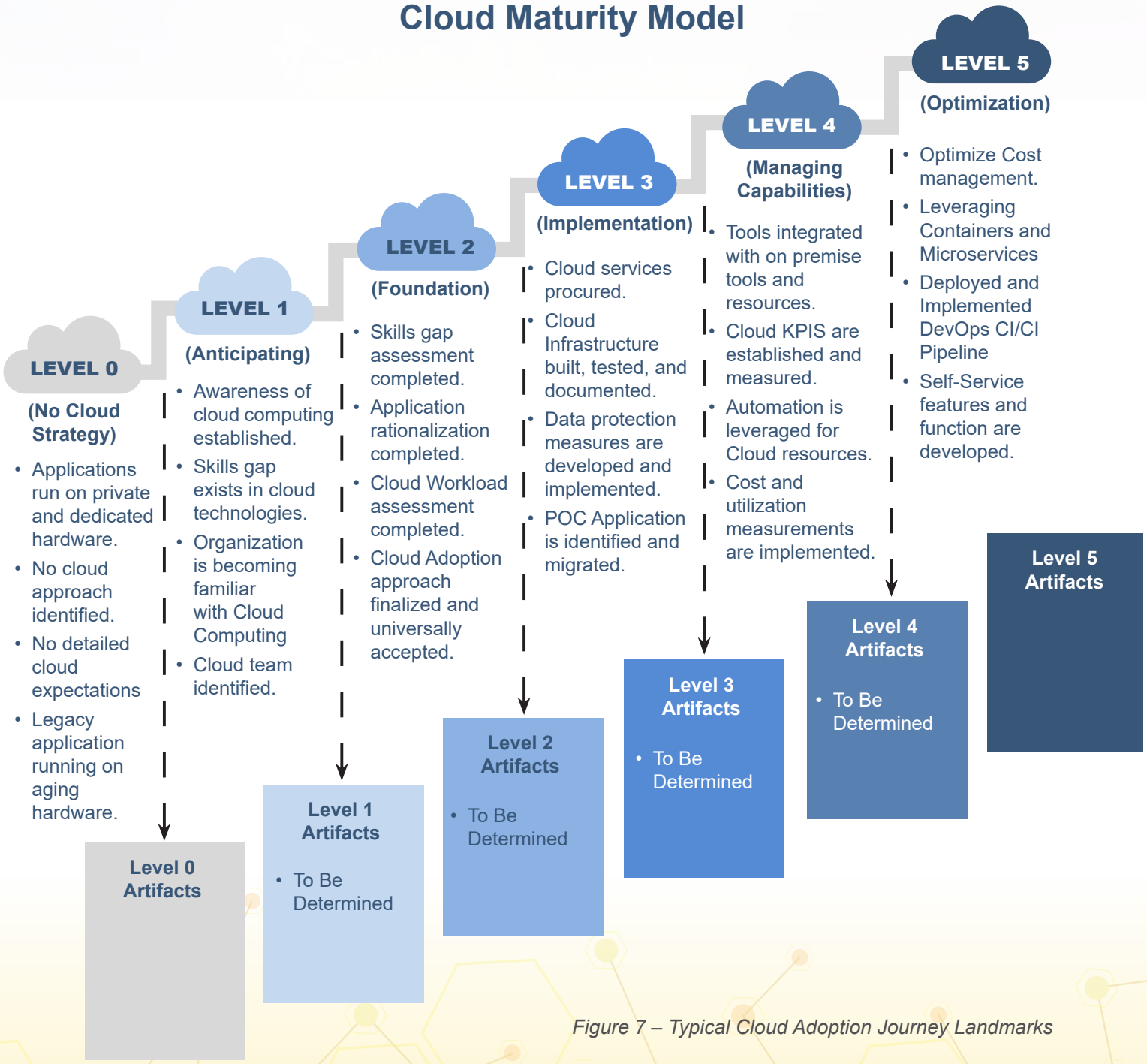


Figure 7 – Typical Cloud Adoption Journey Landmarks

Maturity Level 0 – No Cloud Strategy

If you are just getting started with the cloud, you're at **Maturity Level 0 – No Cloud Strategy**. Typical attributes, action items and artifacts associated with **Maturity Level 0 – No Cloud Strategy** are:

Attributes

- Applications run on private and dedicated hardware.
- No cloud approach identified.
- No detailed cloud expectations.
- Legacy application running on aging hardware.
- Dependent on lengthy procurement process.
- Limited knowledge of Cloud services.
- Limited executive support.
- Organizational cultural challenges to change.

Action Items

- Create Sandbox accounts in CSP environments.
- Collaborate with colleagues who have cloud experience.
- Read articles on Cloud computing technology.
- Begin to have conversations within your organization about concerns or objections to adopting cloud technologies.
- Meet with executives and discuss their views on cloud computing and how it can benefit the organization.
- Document the timeline for procuring hardware and software to compare to the timeline for cloud services.
- Identify the members of your cloud team, this is the group that will manage the cloud adoption and develop the cloud strategy for your organization.

Maturity Level 1 – Anticipating

Maturity Level 1 - Anticipating of cloud adoption maturity affirms an organization has documented and understands their current environment's cloud readiness and has mapped future cloud services to business needs. The business case allows the organization to outline business drivers associated with the strategy. Awareness of cloud computing initiatives are socialized organizationally, and individual divisions have begun to research cloud services however there is no central cloud adoption theme established. Attributes, Actions, and Artifacts associated with **Maturity Level 1 – Anticipating** are:

Attributes

- Awareness of cloud computing established.
- Skills gap exists in cloud technologies.
- Organization is becoming familiar with Cloud Computing.
- No identified business cases for cloud adoption.
- Teams begin researching CSP feature sets and capabilities.
- Resource constrained to begin cloud development.
- Lack of clarity for compliance and governance requirements.
- Cost and Budget management requirements not fully defined.
- Incomplete inventory of on-premises workloads.
- Cloud team identified.

Action Items

- Begin to familiarize yourself with the cloud cost models.
- Skills gap assessment performed.
- Work with a vendor or use a tool to identify the entire inventory of your on-premises environment. This should include dependencies, resource requirements and application versions.
- Develop or leverage basic cloud computing training for your organization.

- Familiarize all your stakeholders with some understanding of what this upcoming change involves.
- Schedule meetings with your business units and develop a method to fully understand how they do their business, their processes, their requirements and identify any challenges or obstacle they have with their current environment.
- Collaborate with Business Units on drivers for Cloud Adoption.
- Evaluate your on-premises, existing governance, and compliance requirements. Determine if they can extend to this new cloud environment or if new requirements will need to be developed.
- Develop Cloud Strategy document!
- Use on premise inventory to develop application assessment for cloud migration.
- Review cloud strategy with vendors or strategic partners.
- Develop cloud training resources for your organization.

Artifacts

- TBD

Maturity Level 2 – Foundation

Maturity Level 2 - Foundation landmark activities turn to bringing clarity of the business case and the associated strategy takes center stage. This maturity level allows an organization to establish a clear path of cloud adoption, prioritize business capabilities and workloads appropriately and define cloud adoption processes. The outcomes of this level of maturity lead to completion of the cloud strategy document, skills gap assessment, developing a design, self-service portal, automation, orchestration, and possibly establishing hybrid cloud models. Attributes, Actions and Artifacts associated with **Maturity Level 2 – Foundation** are:

Attributes

- Skills gap assessment completed.
- Application rationalization completed.
- Cloud Workload assessment completed.
- Cloud Adoption approach finalized and universally accepted.
- Vetted Cloud strategy with vendors and/or strategic partners.
- Review cloud strategy with executive sponsors and business unit stakeholders.
- Cloud strategy document completed.
- On premise workload inventory completed.
- Identify workloads that can be offloaded to SaaS offerings.
- Organizational Cloud training sessions are developed.
- Governance plan developed.

Action Items

- Collaborate with vendors and strategic partners on cloud reference architectures.
- Develop cloud infrastructure architecture.
- Develop cloud tagging policy.
- Create test criteria for cloud POC workload migration.
- Procure cloud account with preferred CSP.
- Develop or leverage existing document control process for cloud infrastructure.
- Classify identified applications as Test/Dev/UAT/Production.
- Identify POC application to migration.
- Develop or extend on premise data protection and monitoring process to cloud environments.

Artifacts

- TBD

Maturity Level 3 – Implementation

Maturity Level 3 – Implementation organizational tools and techniques are interoperable and well-integrated. Automated business and technical services exist, architectural design patterns exist and are used. The cloud adoption plans, and approach has been integrated and implemented into organizational operations. Attributes, Actions, and Artifacts associated with **Maturity Level 3 – Implementation** are:

Attributes

- Cloud services procured.
- Cloud Infrastructure built, tested, and documented.
- Data protection measures are developed and implemented.
- POC Application is identified and migrated.
- Test/Dev/UAT and Production workloads are migrated or refactored in the cloud.
- Workloads properly tagged.

Action Items

- Review current change management process and adjust as need be to accommodate cloud workloads and infrastructure.
- Schedule regular recurring meetings with Cloud strategy team to discuss continual service improvement initiatives. Establish alerts and thresholds for monitoring cost and utilization of cloud workload resources.
- Research cloud automation tools.
- Evaluate if your current on-premises automation tools can be extended to the cloud environment.
- Develop automation processes to create efficiency in your cloud environment.
- Develop Key Performance Indicators and other metrics to measure the efficiency and health of the cloud environment.
- Evaluate your on-premises tool and utilities and determine if they can be extended to your cloud environment of if new tools need to be procured.
- Develop, test, and document your day 2 and M&O operations.
- Migrate Test/Dev/UAT/Production workloads to the cloud.

Artifacts

- TBD

Maturity Level 4 – Managing Capabilities

Maturity Level 4 – Managing Capabilities affirms cloud KPI's are established and measured, automation for cloud resources is leveraged and a change management process is implemented. Business Capabilities are based on human-centered design approaches. API's, platforms, micro-services, and data technologies reduce effort and accelerate service delivery. Attributes, Actions, and Artifacts associated with **Maturity Level 4 – Managing Capabilities** are:

Attributes

- Tools integrated with on premise tools and resources.
- Cloud KPIS are established and measured.
- Automation is leveraged for Cloud resources.
- Cost and utilization measurements are implemented.
- Proactive incident remediation is implemented.
- Change management process implemented.
- Regular Cloud Strategy Committee meetings are convened.

Action Items

- Create a process to research and develop emerging technologies.
- Collaborate with vendors and strategic partners to develop DevOps CI/CD pipeline.
- Evaluate DevOps tools.
- Research and develop self-service options leveraging automation and orchestration built in previous maturity levels.
- Evaluate applications for fit into PaaS or SaaS offerings for maximum efficiently and cost savings.

Artifacts

- TBD

Maturity Level 5 – Optimization

Maturity Level 5 - Optimization affirms the journey is complete – for now. At this point business is focused on the future and actively following optimized innovative trends using cloud technologies. Here the organization is likely federated, interoperable and continually optimizing and improving business delivery leveraging technological means. Attributes, Actions, and Artifacts associated with **Maturity Level 5 - Optimization** are:

Attributes

- Optimize Cost management.
- Leveraging Containers and Microservices.
- Deployed and Implemented DevOps CI/CI Pipeline
- Self-Service features and function are developed.
- Continuous Service improvement process implemented.
- Leverage PaaS services.

Action Items

- Continue to innovate.
- Continue to evaluate evolving business needs and requirements.
- Continue to evaluate emerging technologies.
- Continue to develop training internally or leverage external training resources.

California Department of Technology
703 3rd Street • West Sacramento
California 95605